

WHAT IS CLAIMED IS:

1 1. A method for use in cable systems, the method for forwarding
2 messages containing cryptographic keys from one or more access sytems that control a
3 population of set-top boxes to an encryption renewal system, the method comprising:
4 storing a fictitious address of a virtual set-top box;
5 generating a first message based on the fictitious address, the message
6 containing a first cryptographic key; and
7 forwarding the first message to the fictitious address of the virtual set-top box.

1 2. The method of claim 1 further comprising receiving the first message
2 by the encryption renewal system which has information regarding the fictitious address.

1 3. The method of claim 2 further comrising deriving by the encryption
2 renewal system the first cryptographic key from the first message.

1 4. The method of claim 3 further comprising forwarding to a subscriber
2 set-top box, a control message containing information having the first cryprographic key for
3 allowing the set-top box to decrypt the pre-encrypted content for a designated duration.

1 5. The method of claim 1 wherein the steps of storing, generating and
2 forwarding are performed by a first conditional access system.

1 6. The method of claim 5 wherein the virtual set-top box appears to the
2 first conditional access system as one of the population of set-top boxes within its control.

1 7. The method of claim 5 further comprising,
2 storing, by a second conditional access system, the fictitious address of the
3 virtual set-top box;
4 generating, by the second conditional access system, a second message having
5 a second cryptographic key; and
6 forwarding, by the second conditional access system, the second message to
7 the fictitious address.

1 8. The system of claim 7 wherein the first and second conditional access
2 systems forward the first and second control messages to the same virtual set-top box.

1 9. A conditional access system controlling a population of set-top boxes,
2 the conditional access system comprising:
3 one or more software instructions for storing a virtual set-top box address
4 appearing as part of the population of set-top boxes;
5 one or more software instructions for generating an entitlement management
6 message having a periodical key for controlling both the population of set-top boxes and the
7 virtual set-top box; and
8 one or more software instructions for forwarding the entitlement management
9 message to the virtual set-top box address.

1 10. The conditional access system of claim 9 wherein the virtual set-top
2 box address is unique and no collisions occur with addresses of the population of set-top
3 boxes.

1 11. An encryption renewal system, comprising:
2 one or more software instructions for storing information relating to a virtual
3 set-top address;
4 one or more software instructions for receiving from a first conditional access
5 system a first entitlement management message having a cryptographic key, the entitlement
6 management message being intended for receipt by the virtual set-top address; and
7 one or more software instructions for deriving the cryptographic key from the
8 entitlement management message.

1 12. The encryption renewal system of claim 11 further comprising one or
2 more software instructions for determining that the entitlement management message is from
3 the first conditional access system.

1 13. The encryption renewal system of claim 11 wherein the cryptographic
2 key is a first periodical key through which the first conditional access system controls a first
3 population of set-top boxes.

1 14. The encryption renewal system of claim 11 further comprising
2 one or more software instructions for receiving from a second conditional
3 access system a second entitlement management message having a cryptographic key, the
4 entitlement control message being intended for receipt by the virtual set-top address; and

5 one or more software instructions for deriving the cryptographic key from the
6 entitlement control message.

1 15. The encryption renewal system of claim 13 further comprising a
2 second periodical key through which the second conditional access system controls a second
3 population of set-top boxes.

1 16. The encryption renewal system of claim 13 further comprising a
2 database associated with the first conditional access system of a first video on demand
3 system, and a second conditional access system of a second video on demand system.

1 17. The encryption renewal system of claim 13 further comprising a
2 database for storing the first periodical key of the first conditional access system, and for
3 storing a second periodical key of a second conditional access system.

1 18. A conditional access system controlling a population of set-top boxes,
2 the conditional access system comprising:

3 means for storing a virtual set-top box address which appears as part of the
4 population of set-top boxes;

5 means for generating an entitlement management message having a periodical
6 key through which the conditional access system controls the population of set-top boxes;
7 and

8 means for forwarding the entitlement management message to the virtual set-
9 top box address.

1 19. The conditional access system of claim 9 wherein the virtual set-top
2 box address is unique to prevent collisions.

1 20. An encryption renewal system, comprising:

2 means for storing information relating to a virtual set-top address;

3 means for receiving from a first conditional access system, a first entitlement
4 management message having a cryptographic key, the entitlement control message being
5 intended for receipt by the virtual set-top address; and

6 means for deriving the cryptographic key from the entitlement management
7 message.

1 21. The encryption renewal system of claim 11 further comprising means
2 for determining that the entitlement management message is from the first conditional access
3 system.

1 22. A system for denying access to second pre-encrypted content
2 generated by a compromised off-line encryption device, the system comprising:
3 the off-line encryption device having one or more software instructions for
4 encrypting content to form a first pre-encrypted content and an associated first encryption
5 record having a first time stamp; and
6 an encryption renewal system having
7 one or more software instructions for receiving a signal indicating the
8 first time stamp as a last authorized time stamp,

9 one or more software instructions for receiving a request to access the
10 second pre-encrypted content, the request being accompanied by a second encryption record
11 having a second time stamp; and

12 one or more software instructions for determining whether the second
13 time stamp predates or is contemporaneous to the first time stamp, if yes, granting the request
14 to access the second pre-encrypted content, and if the second time stamp is subsequent to the
15 first time stamp, denying the request to access the second pre-encrypted content.

1 23. The system of claim 22 wherein the request is for an entitlement
2 control message having information about a periodical key for accessing the second pre-
3 encrypted content.

1 24. An encryption renewal system for controlling access to pre-encrypted
2 content generated by an encryption device, the system comprising:

3 one or more software instructions for receiving a request to retrofit an
4 entitlement control message that allows a home device to access pre-encrypted content;

5 one or more software instructions for retrofitting the entitlement control
6 message only after verifying that the pre-encrypted content was generated prior to or
7 contemporaneous with a first authorized timestamp.

1 25. The encryption renewal system of claim 24 wherein the request for the
2 entitlement control message is accompanied by an encryption record having a second time
3 stamp.

1 26. The encryption renewal system of claim 25 wherein the second time
2 stamp indicates when the pre-encrypted content was generated.

1 27. An encryption renewal system for controlling access to pre-encrypted
2 content generated by an encryption device, the system comprising:
3 means for receiving a request for an entitlement control message that allows a
4 home device to access pre-encrypted content;
5 means for generating the entitlement control message only after verifying that
6 the pre-encrypted content was generated prior to or contemporaneous with a first authorized
7 timestamp.

1 28. The encryption renewal system of claim 22 wherein the first
2 encryption record is secured by a cryptographic signature.

1 29. An offline encryption device comprising:
2 one or more software instructions for generating a first time stamp marking
3 when a first encrypted content is generated; and
4 one or more software instructions for generating a second time stamp marking
5 when a second encrypted content is generated, such that if the first time stamp is last
6 authorized, the second encrypted content is decrypt-able only if the second time stamp is
7 prior to or contemporaneous with the first time stamp.

1 30. The system of claim 29 further comprising one or more software
2 instructions for generating an encryption record having the first time stamp.

1 31. The system of 29 further comprising an encryption renewal system for
2 receiving a signal providing that the first time stamp is the last authorized time stamp.

1 32. The system of claim 30 further comprising a video on demand system
2 for forwarding a request to the encryption renewal system to access the second encrypted
3 content.

1 33. The system of claim 32 wherein the request is for an entitlement
2 control message for retrofitting the second encrypted content.

1 34. An offline encryption device comprising:

means for generating a first time stamp marking when a first encrypted content is generated; and

means for generating for generating a second time stamp marking when a second encrypted content is generated, such that if the first time stamp is last authorized, the second encrypted content is decrypt-able only if the second time stamp is prior to or contemporaneous with the first time stamp.

35. The system of claim 29 further comprising means for generating an encryption record having the first time stamp.

09498136 070201
10E020 9E186860